

(OGC/PCLU (Rev. 07/06/2010))

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

(Equivalent to the DOJ Initial Privacy Assessment (IPA))

NAME OF SYSTEM / PROJECT: Consolidated Asset Tracking System (CATS) [REDACTED]

b7E

BIKR FBI Unique Asset ID: N/A

SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Name: [REDACTED]	Name: AGC [REDACTED]
Program Office: Forfeiture and Seized Property Unit	Phone: [REDACTED]
Division: Finance	Room Number: 7350 JEH
Phone: [REDACTED]	
Room Number: WB-510	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: ITOD	Signature: [REDACTED] Date signed: 12-15-10 Name: [REDACTED] Title: IT Specialist	Signature: [REDACTED] Date signed: 11-30-10 Name: [REDACTED] Title: IT Specialist
FBIHQ Division: Finance	Signature: [REDACTED] Date signed: 12-2-10 Name: [REDACTED] Title: Unit Chief	Signature: [REDACTED] Date signed: 12-3-10 Name: [REDACTED] Title: Unit Chief

b6
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

UNCLASSIFIED

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

_____ PIA is required by the E-Government Act.

_____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? _____ Yes. _____ No

☒ PIA is not required for the following reason(s):

_____ System does not collect, maintain, or disseminate PII.

_____ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).

☒ Information in the system relates to internal government operations.

_____ System has been previously assessed under an evaluation similar to a PIA.

☒ No significant privacy issues (or privacy issues are unchanged).

The only PII maintained is the user ID; maintained only within audit logs to which access is limited.

_____ Other

Applicable SORN(s): FBI-002 (Central Records System) and DOJ-002 (DOJ Computer Systems Activity & Access Records)

Notify FBI RMD/RIDS per MIOG 190.2.3? ☒ No _____ Yes--See sample EC on PCLU intranet website here:
http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? ☒ No _____ Yes

Prepare/revise/add Privacy Act (e)(3) statements for related forms? _____ No _____ Yes

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

Elizabeth Withnell, Acting Deputy General Counsel
Acting FBI Privacy and Civil Liberties Officer

Signature:
Date Signed:

Elizabeth Withnell 1/13/10

UNCLASSIFIED

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

The FBI operates the Consolidated Asset Tracking System [REDACTED] (CATS) [REDACTED] the FBINET with the Department of Justice Data Center in Rockville, MD. [REDACTED]

[REDACTED] FBINET is the FBI's secure internal network, accredited to operate at the SECRET classification level. [REDACTED]

b7E

[REDACTED] The CATS [REDACTED] permits FBI personnel to [REDACTED]

[REDACTED] information from the DOJ Consolidated Asset Forfeiture System (CATS). CATS contains information about assets that have been confiscated from individuals participating in criminal activity.

[REDACTED] such as the one utilized by CATS [REDACTED]

b7E

[REDACTED] CATS [REDACTED]

[REDACTED] In the case of CATS [REDACTED]

b7E

[REDACTED] CATS [REDACTED]

[REDACTED] CATS [REDACTED]

CATS [REDACTED]

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

..... NO

...X... YES

Users must sign-in to the CATS ☐ using a user ID and password. The only information maintained by CATS ☐ user ID, date/time of access, and ☐ This information is maintained only in the audit logs for CATS ☐ access to the audit logs is limited to personnel with a need-to-know.

b7E

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

_____ The information directly identifies specific individuals.

_____ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

 X The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

_____ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly.

4. Does the system/project pertain only to government employees, contractors, or consultants?

_____ NO X YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO. [If no, skip to question 7.]

 X YES. [If yes, proceed to the next question.]

CATS ☐ audit logs may be queried via personal identifier (in this case, an individual's user ID). As noted above, access to the audit logs is limited to personnel with a need-to-know.

b7E

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO [If no, proceed to question 7.]

X YES Individual users enter their unique user ID into CATS ☐ where the information is maintained as part of its audit log.

b7E

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

 X NO

 YES [If yes, proceed to question 7.]

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

 X NO

A Privacy Act (e)(3) statement is unnecessary since the user ID in CATS ☐ does not convey information *about* an individual.

b7E

 YES Identify any forms, paper or electronic, used to request such information from the information subject:

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

 X NO YES If yes, check all that apply:

 SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

 SSNs are necessary to identify FBI personnel in this internal administrative system.

 SSNs are important for other reasons. Describe:

 The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). Describe:

 It is not feasible for the system/project to provide special protection to SSNs. Explain:

8. Is the system operated by a contractor?

☒ No.

☐ Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

☐ NO If no, indicate reason; if C&A is pending, provide anticipated completion date:

☒ YES If yes, please indicate the following, if known:

Provide date of last C&A certification/re-certification:

The last certification for CATS ☐ was dated November 29, 2010.

b7E

Confidentiality: ☐ Low ☐ Moderate ☒ High ☐ Undefined

Integrity: ☐ Low ☒ Moderate ☐ High ☐ Undefined

Availability: ☐ Low ☒ Moderate ☐ High ☐ Undefined

☐ Not applicable -- this system is only paper-based.

10. Is this system/project the subject of an OMB-300 budget submission?

☒ NO

☐ YES If yes, please provide the date and name or title of the OMB submission:

11. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

☒ NO

☐ YES If yes, please describe the data mining function:

12. Is this a national security system (as determined by the SecD)?

☒ NO ☐ YES

13. Status of System/ Project:

☐ This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? January 2006

2. Has the system/project undergone any significant changes since April 17, 2003?

☒ NO [If no, proceed to next question (II.3).]

☐ YES If yes, indicate which of the following changes were involved (**mark all changes that apply, and provide brief explanation for each marked change**):

☐ A conversion from paper-based records to an electronic system.

☐ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

☐ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

☐ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

☐ A new method of authenticating the use of and access to information in identifiable form by members of the public.

☐ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

☐ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

☐ A change that results in a new use or disclosure of information in identifiable form.

☐ A change that results in new items of information in identifiable form being added into the system/project.

UNCLASSIFIED

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other [Provide brief explanation]:

3. Does a PIA for this system/project already exist?

_____X_____ NO _____ YES

If yes:

a. Provide date/title of the PIA:

b. Has the system/project undergone any significant changes since the PIA?

_____ NO _____ YES

UNCLASSIFIED

(OGC/PCLU (Rev. 04/01/2011))

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

[Redacted]

b7E

BIKR FBI Unique Asset ID: APP-4000292

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: MAPA [Redacted]	Name: AGC [Redacted]
Reason:	Program Office: Internal Advisory Group	Phone: [Redacted]
Declassify On:	Division: RPO	Room Number: 7350 JEH
	Phone: [Redacted]	
	Room Number: 6256	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Resource Planning Office	Signature: [Redacted] Date signed: 8/24/12 Name: [Redacted] Title: Unit Chief, Internal Advisory Group	Signature: Date signed: Name: Title:
FBIHQ Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

UNCLASSIFIED

UNCLASSIFIED

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

<input type="checkbox"/> PIA is required by the E-Government Act.	
<input type="checkbox"/> PIA is to be completed as a matter of FBI/DOJ discretion.	
Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? <input type="checkbox"/> Yes. <input type="checkbox"/> No (indicate reason):	
<input checked="" type="checkbox"/> PIA is not required for the following reason(s):	
<input type="checkbox"/> System does not collect, maintain, or disseminate PII.	
<input type="checkbox"/> System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).	
<input checked="" type="checkbox"/> Information in the system relates to internal government operations.	
<input type="checkbox"/> System has been previously assessed under an evaluation similar to a PIA.	
<input type="checkbox"/> No significant privacy issues (or privacy issues are unchanged).	
<input checked="" type="checkbox"/> Other (describe): The PII contained in [redacted] is limited to the names of Case Agents responsible for specific [redacted]	
Applicable SORN(s): <u>Accounting Systems for the Department of Justice, JUSTICE-DOJ-001, 69 Fed. Reg. 31406 (June 3, 2004), as modified at 71 Fed. Reg. 142 (Jan. 3, 2006); DOJ Computer Systems Activity and Access Records, JUSTICE/DOJ-002, 64 Fed. Reg. 73585 (Dec. 30, 1999).</u>	
Notify FBI RMD/RIDS per MIOG 190.2.3? <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd	
SORN/SORN revision(s) required? <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes (indicate revisions needed):	
Prepare/revise/add Privacy Act (e)(3) statements for related forms? <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes (indicate forms affected):	
RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.	
Other:	
[redacted] Acting Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 10/26/2012
Christine M. Costello, Acting Deputy General Counsel and Privacy and Civil Liberties Officer	Signature: [redacted] Date Signed: 10/24/12

b7E

b6
b7C

UNCLASSIFIED

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

[redacted]
[redacted] permits the FBI to accurately track [redacted]
[redacted]

b7E

[redacted] eliminates the administrative burden of [redacted]
[redacted]

b7E

Due to various organizational or operational reasons [redacted]
[redacted]
[redacted] Prior to [redacted] FBI
personnel would have to manually [redacted]
[redacted]

b7E

[redacted]
[redacted] The use of [redacted] should lead to increased

b7E

[redacted]

b7E

accuracy and ease in [REDACTED]
[REDACTED]

b7E

The PII contained in [REDACTED] is limited to the names and division assignments of Case Agents responsible for [REDACTED] and user information (name and user name) necessary for [REDACTED] and system security review. Access to user information is limited to developers and individuals with privileged user roles such as administrators and account managers. Access to [REDACTED] is restricted to personnel in RPO's Internal Advisory Group (who also serve as system administrators), a limited number of FBI [REDACTED] personnel at Field Offices and FBIHQ, and personnel responsible for system security.

b7E

As an [REDACTED] is not separately accredited. [REDACTED] resides on the FBI Enterprise Servers (ES) and is encompassed by the ES C&A. Pending approval of a separate System Security Plan (SSP) for [REDACTED] its access and audit logs are generated and reviewed in accordance with the ES SSP.

b7E

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

 NO

 X YES [If yes, please continue.]

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

 X The information directly identifies specific individuals.

 The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

 X The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

 None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly.

4. Does the system/project pertain only to government employees, contractors, or consultants?

 NO X YES

UNCLASSIFIED

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

☒ NO. [If no, skip to question 7.]

☐ YES. [If yes, proceed to the next question.]

6. Does the system/project collect any information directly from the person who is the subject of the information?

☒ NO [If no, proceed to question 7.]

☐ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

☐ NO

☒ YES [If yes, proceed to question 7.]

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

☐ NO [The program will need to work with PCLU to develop/implement the necessary form(s).]

☐ YES Identify any forms, paper or electronic, used to request such information from the information subject:

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

☒ NO ☐ YES If yes, check all that apply:

☐ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

☐ SSNs are necessary to identify FBI personnel in this internal administrative system.

☐ SSNs are important for other reasons. Describe:

UNCLASSIFIED

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

8. Is the system operated by a contractor?

 X No.

_____ Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

_____ NO If no, indicate reason; if C&A is pending, provide anticipated completion date:

 X YES If yes, please indicate the following, if known:

Provide date of last C&A certification/re-certification:

resides on the Enterprise Server (ES) and is encompassed by the C&A for ES. The ES was most recently accredited on December 16, 2012 and has authority to operate (ATO) though December 16, 2012 at the following risk levels.

b7E

Confidentiality: ___ Low X Moderate ___ High

Integrity: ___ Low X Moderate ___ High

Availability: ___ Low X Moderate ___ High

_____ Not applicable -- this system is only paper-based.

10. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

UNCLASSIFIED

X NO

____ YES If yes, please describe the data mining function:

11. Is this a national security system (as determined by the SecD)?

X NO _____ YES

12. Status of System/ Project:

X This is a new system/project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

____ NO [If no, proceed to next question (II.3).]

____ YES If yes, indicate which of the following changes were involved (mark all changes that apply, and provide brief explanation for each marked change):

____ A conversion from paper-based records to an electronic system.

____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

UNCLASSIFIED

UNCLASSIFIED

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other [Provide brief explanation]:

3. Does a PIA for this system/project already exist?

_____ NO _____ YES

If yes:

a. Provide date/title of the PIA:

b. Has the system/project undergone any significant changes since the PIA?

_____ NO _____ YES

UNCLASSIFIED

(OGC/PCLU (Rev. 04/01/2011))

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [REDACTED]

b7E

BIKR FBI Unique Asset ID: N/A

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [REDACTED] Program Office: Crimes Against Children Unit Division: CID Phone: [REDACTED] Room Number: JEH, Rm G-300	FBI OGC/PCLU POC Name: [REDACTED] Phone: [REDACTED] Room Number: JEH, Rm 7350
--------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Crimes Against Children	Signature: [REDACTED] Date signed: 12/29/2011 Name: [REDACTED] Title: Unit Chief	Signature: [REDACTED] Date signed: 1/29/2012 Name: [REDACTED] Title: Special Assistant to the Assistant Director
FBIHQ Division: Criminal Investigative Division	Signature: [REDACTED] Date signed: 1/18/2012 Name: [REDACTED] for [REDACTED] Title: Assistant Section Chief	Signature: [REDACTED] Date signed: 1/29/2012 Name: [REDACTED] Title: Special Assistant to the Assistant Director

b6
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the
following page.)

UNCLASSIFIED//FOUO

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

☒ PIA is required by the E-Government Act.

☐ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ☒ Yes. ☐ No:

☐ PIA is not required for the following reason(s):

☐ System does not collect, maintain, or disseminate PII.

☐ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).

☐ Information in the system relates to internal government operations.

☐ System has been previously assessed under an evaluation similar to a PIA.

☐ No significant privacy issues (or privacy issues are unchanged).

☐ Other :

Applicable SORN(s): Central Records System, DOJ/FBI-002

Notify FBI RMD/RIDS per MIOG 190.2.3? ☐ No ☒ Yes--See sample EC on PCLU intranet website here:
http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? ☒ No ☐ Yes :

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ☐ No ☐ Yes :

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

Unit Chief
Privacy and Civil Liberties Unit

Signature:

Date Signed: 01/21/2011

James J. Landon, Deputy General Counsel
FBI Privacy and Civil Liberties Officer

Signature: [Signature]

Date Signed: 01/27/11

b6
b7c

UNCLASSIFIED//FOUO

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

[redacted] is an internet-accessed database [redacted] It will be accessible to FBI employees [redacted] already used by the FBI for other tools). Each user has a unique username and password that allows the individual to sign-in to the web-based application [redacted] does not connect to any other database.

b7E

[redacted] will be used by FBI personnel during child abduction investigations [redacted]

b7E

Information within [redacted] includes [redacted]

b7E

b7E

[redacted] will allow users to filter search results by [redacted] [redacted] Users will be able to obtain a comprehensive report [redacted] and the report will contain additional information [redacted]

b7E

¹ This tool will replace the ReSOLI tool, previously used in child abduction cases.

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

_____ NO

 X YES [If yes, please continue.]

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

 X The information directly identifies specific individuals.

 X The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

 X The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

_____ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly.

4. Does the system/project pertain only to government employees, contractors, or consultants?

 X NO _____ YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO. [If no, skip to question 7.]

 X YES. [If yes, proceed to the next question.]

6. Does the system/project collect any information directly from the person who is the subject of the information?

 X NO [If no, proceed to question 7.]

☐ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

☐ NO

☐ YES [If yes, proceed to question 7.]

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

☐ NO [The program will need to work with PCLU to develop/implement the necessary form(s).]

☐ YES Identify any forms, paper or electronic, used to request such information from the information subject:

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

☐ NO ☒ YES If yes, check all that apply:

☒ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

☐ SSNs are necessary to identify FBI personnel in this internal administrative system.

☐ SSNs are important for other reasons. Describe:

☒ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). Describe: The tool masks the first five digits of an individual's SSN. However, any individual may view the entire SSN by

b7E

☐ It is not feasible for the system/project to provide special protection to SSNs. Explain:

8. Is the system operated by a contractor?

☐ No.

☒ Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

☒ NO If no, indicate reason; if C&A is pending, provide anticipated completion date: Security Division has determined that C&A is not required for the use of this tool.

☐ YES If yes, please indicate the following, if known:

Provide date of last C&A certification/re-certification:

Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

☐ Not applicable – this system is only paper-based.

10. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

☒ NO

☐ YES If yes, please describe the data mining function:

11. Is this a national security system (as determined by the SecD)?

☒ NO

☐ YES

12. Status of System/ Project:

☒ This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

_____ YES If yes, indicate which of the following changes were involved **(mark all changes that apply, and provide brief explanation for each marked change):**

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

UNCLASSIFIED//FOUO

_____ Other [Provide brief explanation]:

3. Does a PIA for this system/project already exist?

_____ NO _____ YES

If yes:

a. Provide date/title of the PIA:

b. Has the system/project undergone any significant changes since the PIA?

_____ NO _____ YES

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOR OFFICIAL USE ONLY
FBI PTA: Continuity Management System (CMS)

(OGC/PCLU (Rev. 08/16/2010))

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Continuity Management System (CMS)

BIKR FBI Unique Project ID: 2010-016-01-P-302-094-9999

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: ITS [REDACTED]	Name: AGC [REDACTED]
Reason:	Program Office: System Support Section	Phone: [REDACTED]
Declassify On:	Division: Information Technology	Room Number: 7350 JEH
	Services Division (ITSD)	
	Phone: [REDACTED]	
	Room Number: JEH 1907	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: ITSD	Signature: [REDACTED] Date signed: 6/10/2011 Name: [REDACTED] Title: CMS PM	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: [REDACTED]
FBIHQ Division: ITSD	Signature: [REDACTED] Date signed: 6/15/2011 Name: [REDACTED] Title: Assistant Section Chief, System Support Section	Signature: [REDACTED] Date signed: 7-15-11 [REDACTED] Name: [REDACTED] Title: IT Specialist, ITB Privacy Officer

b6
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).

(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY
FBI PTA: Continuity Management System (CMS)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

____ PIA is required by the E-Government Act.

____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ____ Yes. ____ No (indicate reason):

X PIA is not required for the following reason(s):

____ System does not collect, maintain, or disseminate PII.

____ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).

X Information in the system relates to internal government operations.

____ System has been previously assessed under an evaluation similar to a PIA.

____ No significant privacy issues (or privacy issues are unchanged).

____ Other (describe):

Applicable SORN(s): N/A

FBI COOP plans are maintained by the Security Division within case category 319Q-HQ-A1487664, *Emergency Plans*.

Notify FBI RMD/RIDS per MIOG 190.2.3? X No ____ Yes--See sample EC on PCLU intranet website here:

http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? X No ____ Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? X No ____ Yes (indicate forms affected):

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

____ Unit Chief
Privacy and Civil Liberties Unit
James J. Landon, Deputy General Counsel/
FBI Privacy and Civil Liberties Officer

Signature: _____

Date Signed: _____

Signature: _____

Date Signed: _____

b6
b7C

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FBI PTA: Continuity Management System (CMS)

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

Continuity of operations plans (COOPs) are federally-mandated plans to ensure that the United States government continues to provide mission essential services to the American public during any type of emergency or disaster, whether natural or man-made. National Security Presidential Directive (NSPD) 51/Homeland Security Presidential Directive (HSPD) 20 requires Executive Branch departments and agencies to develop and maintain COOPs in support of National Essential Functions (NEFs). Within the FBI, Corporate Policy Directive (CPD) 0210D, *Continuity of Operations (COOP)* (Nov. 17, 2009), requires that the FBI maintain a COOP program to ensure that mission essential functions (MEFs) continue under all circumstances.

To support contingency planning for COOP events, the FBI holds a license for Continuity Management Solution¹ (CMS), a comprehensive commercial-off-the-shelf (COTS) software product developed by SunGard Availability Services designed to help manage the entire lifecycle of a Business Continuity program. CMS utilizes a common platform that enables data consistency across multiple planning, testing and execution-management processes, as well as seamless enterprise reporting.

The FBI will utilize two CMS applications for COOP purposes, the Living Disaster Recovery Planning System (LDRPS) and the Business Impact Analysis Professional (BIA).

LDRPS automates the creation, maintenance, storage and retrieval of COOPs throughout Bureau components (FBI HQ Divisions and Field Offices) through the use of templates and interface tools.² COOPs contained in LDRPS will typically include information regarding:

b7E

¹ Continuity Management System is the internal FBI name for this application and project.

² It is anticipated that the COOPs maintained within LDRPS will initially pertain only to [REDACTED]. As CMS is deployed, individual component COOPs (maintained by the Security Division within case classification 319Q) may also be added to LDRPS.

b7E

FBI PTA: Continuity Management System (CMS)



b7E


The BIA software in CMS will be used to acquire information within the FBI regarding vulnerabilities (such as operational and financial), impacts and recovery strategies. BIA organizes complex data presenting it in a usable format that will assist FBI personnel in creating COOPs.

As a first step, BIA will be used to create internal surveys seeking to identify FBI weaknesses and vulnerabilities. For example, a survey question might ask "[w]hat areas of your Division should receive priority attention during an event triggering a COOP." A CMS administrator will prepare the survey and electronically distribute it to relevant personnel with COOP responsibilities.

BIA also facilitates the review of survey results by appropriate personnel. The scope of survey results available for viewing may range from individual responses within a specific Division to Bureau-wide.

BIA also has a robust reporting function, enabling FBI planners to build customized reports displaying collected data in charts and graphs using such programs as Microsoft Excel. Reports can be saved in PDF format for easy distribution.

CMS will contain limited personally identifiable information (PII) about individuals associated with the LDRPS and BIA applications. This information will include the names and contact information (office, home and Blackberry telephone numbers, Government e-mail address) of FBI personnel designated as members of a COOP Emergency Relocation Group (ERG); names and contact information for FBI vendors (address, telephone number and POC) whose services may be required in a COOP event; and the names and contact information (physical location, telephone number) of FBI personnel participating in BIA surveys. Neither SSNs nor DOBs will be contained in CMS.

CMS will  and will be accessed from FBINET/Secret Enclave workstations. Access to CMS will be restricted to COOP Coordinators within each Headquarters Division and Field Office, as well as one or more system administrators. The system administrator(s) will identify individuals requiring access to CMS and provide those individuals with a link to the CMS site.

b7E

Individual COOP Coordinators will only be able to access and modify the specific COOP plan for which they are responsible; similarly, they will only have access to the BIA surveys pertaining to their specific component. CMS system administrators will, however, have access to all COOP Plans within LDRPS, as well as to all survey results contained in BIA.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FBI PTA: Continuity Management System (CMS)

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

_____ NO [If no, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are otherwise advised, no PIA is required.]

X YES [If yes, please continue.]

While CMS contains point-of-contact (POC) information, the purpose of the system is to collect and maintain COOPs and work associated with those plans.

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

X The information directly identifies specific individuals.

CMS contains POC information for individuals associated with COOP plans and events.

_____ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

X The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals.

If you marked any of the above, proceed to Question 4.

_____ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly. [If you checked this item, STOP here after providing the requested description.]

4. Does the system/project pertain only to government employees, contractors, or consultants?

_____ NO X YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

X NO. [If no, skip to question 7.]

_____ YES. [If yes, proceed to the next question.]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FBI PTA: Continuity Management System (CMS)

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO [If no, proceed to question 7.]

_____ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ NO

_____ YES [If yes, proceed to question 7.]

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO [The program will need to work with PCLU to develop/implement the necessary form(s).]

_____ YES Identify any forms, paper or electronic, used to request such information from the information subject:

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

 X NO _____ YES If yes, check all that apply:

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. Describe:

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). Describe:

_____ It is not feasible for the system/project to provide special protection to SSNs. Explain:

8. Is the system operated by a contractor?

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY
FBI PTA: Continuity Management System (CMS)

 X No.

 Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

 NO If no, indicate reason; if C&A is pending, provide anticipated completion date:

 X YES If yes, please indicate the following, if known:

Since CMS is an application, rather than an IT system, it will not be separately accredited. CMS will [REDACTED] which was accredited on August 31, 2010 and has authority to operate (ATO) through August 30, 2013. [REDACTED] has the following risk levels:

b7E

Confidentiality: Low Moderate X High Undefined

Integrity: Low Moderate X High Undefined

Availability: Low Moderate X High Undefined

 Not applicable -- this system is only paper-based.

10. Is this system/project the subject of an OMB-300 budget submission?

 X NO

 YES If yes, please provide the date and name or title of the OMB submission:

11. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

 X NO

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FBI PTA: Continuity Management System (CMS)

_____ YES If yes, please describe the data mining function:

12. Is this a national security system (as determined by the SecD)?

_____ NO X YES

It is anticipated that at least some of the information contained in COOPs maintained in CMS will contain classified information.

13. Status of System/ Project:

 X This is a new system/ project in development. [If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

_____ YES If yes, indicate which of the following changes were involved (mark all changes that apply, and provide brief explanation for each marked change):

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FBI PTA: Continuity Management System (CMS)

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other [Provide brief explanation]:

3. Does a PIA for this system/project already exist?

_____ NO _____ YES

If yes:

a. Provide date/title of the PIA:

b. Has the system/project undergone any significant changes since the PIA?

_____ NO _____ YES

[The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(OGC/PCLU (Rev. 08/16/2010))

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: COMSEC [REDACTED]

b7E

BIKR FBI Unique Asset ID: SYS-0000017

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: [REDACTED]	Name: AGC [REDACTED]
Reason:	[REDACTED]	Phone: [REDACTED]
Declassify On:	Program Office: Data Communications Security Unit (DCSU)/FBI Central Office of Record (COR) Division: Security Phone: [REDACTED] Room Number: 1B206B	Room Number: 7350 JEH

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: [REDACTED] Date signed: 2/10/2011 Name: Title:	Signature: [REDACTED] Date signed: Name: Title:
FBIHQ Division: Security Division	Signature: [REDACTED] Date signed: 2/10/2011 Name: [REDACTED] Title: Chief, Data Communications Security Unit	Signature: [REDACTED] Date signed: 2/17/11 Name: Brigitte Flynn Class Title: Chief, Mission Support Section

b6
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).

(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

_____ PIA is required by the E-Government Act.

_____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? _____ Yes. _____ No (indicate reason):

☒ PIA is not required for the following reason(s):

_____ System does not collect, maintain, or disseminate PII.

_____ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).

☒ Information in the system relates to internal government operations.

_____ System has been previously assessed under an evaluation similar to a PIA.

_____ No significant privacy issues (or privacy issues are unchanged).

_____ Other (describe):

Applicable SORN(s): Justice/FBI-008, Bureau Personnel and Management System (BPMS)

The official names of Bureau personnel responsible for COMSEC material ☒ contained in is also contained in BPMS.

Notify FBI RMD/RIDS per MIOG 190.2.3? ☒ No _____ Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? ☒ No _____ Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ☒ No _____ Yes

See comments below.

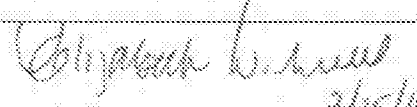
RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

Standard Form 153 (SF-153), *COMSEC MATERIAL REPORT*, is used throughout the United States Intelligence Community, including the FBI, to formally account for custody of COMSEC materials. SF-153 contains the names and signatures of individuals handling COMSEC materials, but does not contain a Privacy Act Statement.

SF-153s pertaining to FBI COMSEC materials are retained by the FBI's Central Office of Record (COR) for five years and then destroyed.

Elizabeth Ross Withnell, Acting Deputy General Counsel and FBI Privacy and Civil Liberties Officer

Signature: 
Date Signed: 2/25/10

b7E

b7E

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

Communications Security (COMSEC) is the protection of classified and sensitive information through electronic systems utilizing cryptographic equipment, documents and aids. One aspect of COMSEC is the use of secure telecommunications and information handling equipment and associated cryptographic components. [REDACTED]

b7E

The Security Division's Data Communications Security Unit (DCSU) has been designated as the FBI's Central Office of Record (COR), responsible for FBI COMSEC materials and equipment. To facilitate its work, COR utilizes the COMSEC [REDACTED]

b7E

[REDACTED] Access to [REDACTED] is restricted to FBI personnel in the COMSEC program.

Only limited personally identifiable information (PII) about FBI personnel is maintained in [REDACTED]. Personnel are identified in [REDACTED] by their name and [REDACTED] user ID. Originally a standalone system operated by COR, [REDACTED] is being added as an application to the FBI's Secret Enclave (FBINET), the Bureau's network for the primary investigative and administrative work of the FBI. Deployment on the Secret Enclave will enable COR, as well as COMSEC managers and alternate managers at HQ and in the field, to [REDACTED]

b7E

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

_____ NO

 X YES [If yes, please continue.]

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.

(Check all that apply.)

 X The information directly identifies specific individuals.

_____ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

☒ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly.

4. Does the system/project pertain only to government employees, contractors, or consultants?

_____ NO ☒ YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO. [If no, skip to question 7.]

☒ YES. [If yes, proceed to the next question.]

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO [If no, proceed to question 7.]

☒ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

☒ NO *not directly*

_____ YES [If yes, proceed to question 7.]

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

☒ NO See comments regarding SF-153 on page 2.

_____ YES

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

☒ NO ☐ YES If yes, check all that apply:

UNCLASSIFIED//FOR OFFICIAL USE ONLY

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. Describe:

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). Describe:

_____ It is not feasible for the system/project to provide special protection to SSNs. Explain:

8. Is the system operated by a contractor?

☒ No.

_____ Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

☒ NO If no, indicate reason; if C&A is pending, provide anticipated completion date:

C&A is pending for [] and is expected to be completed in mid-2011. At this time, the anticipated risk levels are "High" in all three categories.

b7E

_____ YES If yes, please indicate the following, if known:

Provide date of last C&A certification/re-certification:

Confidentiality: ___ Low ___ Moderate ___ High ___ Undefined

Integrity: ___ Low ___ Moderate ___ High ___ Undefined

Availability: ___ Low ___ Moderate ___ High ___ Undefined

UNCLASSIFIED//FOR OFFICIAL USE ONLY

..... Not applicable -- this system is only paper-based.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

10. Is this system/project the subject of an OMB-300 budget submission?

☒ NO

☐ YES If yes, please provide the date and name or title of the OMB submission:

11. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

☒ NO

☐ YES If yes, please describe the data mining function:

12. Is this a national security system (as determined by the SecD)?

☐ NO

☐ YES

13. Status of System/ Project:

☐ This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? 2004

2. Has the system/project undergone any significant changes since April 17, 2003?

☐ NO [If no, proceed to next question (II.3).]

☒ YES If yes, indicate which of the following changes were involved (mark all changes that apply, and provide brief explanation for each marked change):

☐ A conversion from paper-based records to an electronic system.

☐ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

☒ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.) The "new use" is

make change from a database to a network system, but access is not enabled.
☐ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

X Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other [Provide brief explanation]:

3. Does a PIA for this system/project already exist?

X NO _____ YES

If yes:

a. Provide date/title of the PIA:

b. Has the system/project undergone any significant changes since the PIA?

_____ NO _____ YES

[The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(OGC/PCLU (Rev. 04/01/2011))

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [REDACTED]

b7E

BIKR FBI Unique Asset ID: PENDING

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: MPA [REDACTED]	Name: AGC [REDACTED]
Reason:	Program Office: Resource Planning Office	Phone: [REDACTED]
Declassify On:	Division: Director's Office (DO)	Room Number: 7350 JEH
	Phone: [REDACTED]	
	Room Number: 6220	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:
FBIHQ Division: Resource Planning Office, Director's Office	Signature: [REDACTED] Date signed: 1/3/2013 Name: [REDACTED] Title: Unit Chief, Resource Planning Office	Signature: Date signed: Name: N/A Title:

b6
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS: [This section will be completed by the FBI PCLU/PCLO following PTA submission. The PTA drafter should skip to the next page and continue.]

☐ PIA is required by the E-Government Act.

☐ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ☐ Yes. ☐ No (indicate reason):

☒ PIA is not required for the following reason(s):

☐ System does not collect, maintain, or disseminate PII.

☐ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).

☒ Information in the system relates to internal government operations.

☐ System has been previously assessed under an evaluation similar to a PIA.

☒ No significant privacy issues (or privacy issues are unchanged).

☐ Other (describe):

Applicable SORN(s): DOJ Computer Systems Activity and Access Records, DOJ-002, 64 Fed. Reg. 73585 (Dec. 30, 1999), as modified at 66 Fed. Reg. 8425 (Jan. 31, 2001) and at 72 Fed. Reg. 3410 (Jan. 25, 2007)

Notify FBI RMD/RIDS per MIOG 190.2.3? ☒ No ☐ Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? ☒ No ☐ Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ☒ No ☐ Yes (indicate forms affected):

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

☐ Acting Unit Chief
Privacy and Civil Liberties Unit

Signature: ☐

Date Signed: 1/3/2013

Christine M. Costello, Acting Deputy General Counsel
and FBI Privacy and Civil Liberties Officer

Signature: 

Date Signed: 1-3-2013

b6
b7c

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

The FBI's Resource Planning Office (RPO), Resource Analysis Unit (RAU), oversees the allocation of all field office special agents and professional staff Funded Staffing Levels (FSLs) through the [REDACTED]. Through announced open seasons, usually occurring annually, field offices are given the opportunity to request additional resources, while headquarters program managers assess long-term personnel resource needs in order to actively address top operational priorities.

b7E

The RPO has developed an application and electronic workflow, the [REDACTED] [REDACTED] for the processing of FSL requests and to provide FBI Senior Executives with information and reports regarding pending or closed resource requests. [REDACTED] is replacing the [REDACTED] [REDACTED] presently used for these purposes. Users in the field and at headquarters will now be able to track FSL resource requests [REDACTED] and resource reports will be automated, which will enhance the efficiency and transparency of the process.

b7E

[REDACTED] will collect resource request information from field offices and automatically forward that information to the relevant division program managers at FBI headquarters. The information collected and maintained in the database will consist of:

b7E

- The name of the Field Office submitting the request;
- The type of the position/subposition (i.e., Agent - MST-A (mobile surveillance team - armed));
- The investigative program/subprograms affected;
- The number of FSLs being requested or recommended; and
- Field Office and HQ Program justifications for the request.

No personally identifiable information (PII) will be collected or maintained by the application, except for the usernames of individuals involved in the submission and processing of resource requests. These users will typically consist of approximately 2-3 individuals within each Field Office, Program Managers assigned to Headquarters Divisions, and RAU personnel. Requests for user privileges must be approved by RAU. Role-based access will also be utilized. Users assigned to field offices and headquarters divisions will have read/write access, while RAU personnel will have administrator roles with read/write/modify privileges and the ability to authorize new user access.

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

☐ NO [If no, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are otherwise advised, no PIA is required.]

☒ YES [If yes, please continue.]

NOTE: the only information about individuals collected, maintained or disseminated from the are the usernames of individuals involved in the resource request process (i.e., submitting, reviewing, revising, commenting on or approving a request).

b7E

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

☒ The information directly identifies specific individuals.

☐ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

☒ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

☐ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly. [If you checked this item, STOP here after providing the requested description.]

4. Does the system/project pertain only to government employees, contractors, or consultants?

☐ NO ☒ YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

☒ NO. [If no, skip to question 7.]

☐ YES. [If yes, proceed to the next question.]

6. Does the system/project collect any information directly from the person who is the

subject of the information?

_____ NO [If no, proceed to question 7.]

_____ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ NO

_____ YES [If yes, proceed to question 7.]

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO [The program will need to work with PCLU to develop/implement the necessary form(s).]

_____ YES Identify any forms, paper or electronic, used to request such information from the information subject:

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

 X NO _____ YES If yes, check all that apply:

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. Describe:

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). Describe:

_____ It is not feasible for the system/project to provide special protection to SSNs. Explain:

8. Is the system operated by a contractor?

☒ No.

Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

☐ NO If no, indicate reason; if C&A is pending, provide anticipated completion date:

☒ YES If yes, please indicate the following, if known:

Provide date of last C&A certification/re-certification: December 16, 2011

The [redacted] will reside on the Enterprise Server (ES) and is encompassed by the ES C&A. The ES was most recently accredited on December 16, 2011 and has authority to operate (ATO) through December 16, 2014 at the following risk levels. The following are the ES risk levels:

b7E

Confidentiality: ☐ Low ☐ Moderate ☒ High ☐ Undefined

Integrity: ☐ Low ☐ Moderate ☒ High ☐ Undefined

Availability: ☐ Low ☐ Moderate ☒ High ☐ Undefined

☐ Not applicable – this system is only paper-based.

10. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

☒ NO

☐ YES If yes, please describe the data mining function:

11. Is this a national security system (as determined by the SecD)?

☒ NO ☐ YES

12. Status of System/Project:

X This is a new system/ project in development. [If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

 NO [If no, proceed to next question (II.3).]

 YES If yes, indicate which of the following changes were involved (mark all changes that apply, and provide brief explanation for each marked change):

 A conversion from paper-based records to an electronic system.

 A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

 A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

 A change that results in information in identifiable form being merged, centralized, or matched with other databases.

 A new method of authenticating the use of and access to information in identifiable form by members of the public.

 A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

 A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

 A change that results in a new use or disclosure of information in identifiable form.

 A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other [Provide brief explanation]:

3. Does a PLA for this system/project already exist?

_____ NO _____ YES

If yes:

a. Provide date/title of the PLA:

b. Has the system/project undergone any significant changes since the PLA?

_____ NO _____ YES

[The PLA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PLA and/or other actions are required.]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(OGC/PCLU (Rev. 01/05/09))

FBI PRIVACY THRESHOLD ANALYSIS (PTA)
(equivalent to the DOJ Initial Privacy Assessment (IPA))

NAME OF SYSTEM / PROJECT: [REDACTED] b7E

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: [REDACTED]	Name:
Reason:	Program Office: Language Services	Phone:
Declassify On:	Division: Directorate of Intelligence	Room Number:
	Phone: [REDACTED]	
	Room Number: WB-603	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS [complete as necessary]

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: [REDACTED] Date signed: 7/15/09 Name: [REDACTED] Title: FL Program Manager	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: [REDACTED]
FBIHQ Division: Directorate of Intelligence	Signature: [REDACTED] Date signed: 7/15/09 Name: Margaret R. Gulotta Title: Section Chief	Signature: [REDACTED] Date signed: 8/16/09 Name: [REDACTED] Title: Unit Chief/Privacy Officer

b6
b7C

Additional division(s) approvals may be added as warranted:

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7338).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

Upon final FBI approval, FBI OGC/PCLU will distribute as follows:

- 1 - Signed original to file 190-HQ-C1321794 (fwd to JEH 1B204 via PA-520)
- Copies (recipients please print/reproduce as needed for Program/Division file(s)):

- 1 - DOJ Office of Privacy and Civil Liberties (via e-mail to privacy@usdoj.gov)
(if classified, via hand delivery to 1331 Penn. Ave. NW, Suite 940, 20530)

- 2 - FBI OCIO / OIPP (JEH 9376, attn: [REDACTED])

- 1 - FBI SecD/AU (electronic copy: via e-mail to UC [REDACTED])

- 1 - RMD/RMAU (attn: [REDACTED])

- 2 - Program Division POC /Privacy Officer

- 2 - FBIHQ Division POC /Privacy Officer

- 1 - OGC/PCLU intranet
- 1 - PCLU UC
- 1 - PCLU Library
- 1 - PCLU Tickler

b6
b7C

UNCLASSIFIED//FOR OFFICIAL USE ONLY